

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*

Case No. 2:22-mj-262

A BLACK KINGSTON 4GB DATA TRAVELER 4000 AND A
BLACK IPHONE 4S, CURRENTLY LOCATED AT 425 W.
NATIONWIDE BLVD., COLUMBUS OHIO, 43215

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See attachment A.

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

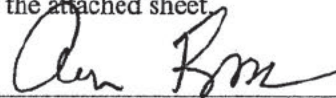
Offense Description

18 U.S.C. §§ 1956, 1957 Money Laundering

The application is based on these facts:

See attached affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Aaron Beggs SPECIAL AGENT

Printed name and title

Sworn to before me and signed in my presence.

Date: April 12, 2022City and state: Columbus, Ohio
Kimberly A. Johnson
United States Magistrate Judge

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO**

IN THE MATTER OF THE SEARCH OF A
BLACK KINGSTON 4GB DATA TRAVELER
4000 AND A BLACK IPHONE 4S, CURRENTLY
LOCATED AT 425 W. NATIONWIDE BLVD.,
COLUMBUS OHIO, 43215

Case No. 2:22-mj-262

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Aaron Beggs, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two electronic devices—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since May 2004. I am currently assigned to the Cincinnati Division Columbus Resident Agency as a member of White-Collar Crimes squad, where I investigate violations of federal law relating to Complex Financial Crimes and Healthcare Fraud. Since becoming an FBI agent, I have received specialized training in computer security as well as on-the-job training investigating criminal activities that include various types of fraud and money laundering. I also have participated in investigations involving violent crime, kidnappings, fugitives, identity theft, extortion, crimes against children, public corruption and domestic terrorism.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is:

- a. a black Kingston 4GB Data Traveler 4000 and
- b. a black Apple iPhone 4s Model: A1387, FCC ID: BCG-E2430A

(collectively, the Devices) which are currently in the custody of the FBI and located in the evidence control room located at 425 W. Nationwide Boulevard, Columbus, Ohio 43215.

5. The applied-for warrant would authorize the forensic examination of the Devices, wherever they may be found, for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On March 3, 2021, Dinsmore & Shohl LLP (Dinsmore) located at 191 Nationwide Blvd., Columbus Ohio 43215, received a priority mail package addressed to Dinsmore but without a specific individual identified. Dinsmore mailroom employees opened the package and noticed it contained an envelope of \$100 dollar bills. Shortly after the package arrived, Dinsmore records clerk [REDACTED], went to the mailroom and requested a priority

mail envelope. The mailroom employees asked [REDACTED] to describe the contents of the package. [REDACTED] replied "a lot of green." Mailroom employees released the package to [REDACTED]

7. On March 4, 2021, [REDACTED] told Dinsmore Law Firm Partner [REDACTED] the package contained \$1,000. Following this receipt, [REDACTED] sent this money to an individual named [REDACTED]

8. On the morning of March 4, 2021, Dinsmore received a call from a woman named [REDACTED] requested the return of her friend [REDACTED] money. [REDACTED] told [REDACTED] that Alabama resident [REDACTED] sent \$12,000 to [REDACTED] at Dinsmore. [REDACTED] sent the money to [REDACTED] at the request of [REDACTED] was the individual [REDACTED] had sent money to in the past. [REDACTED] informed [REDACTED] he needed money to get a "helicopter off of an oil rig." [REDACTED] believed her friend had been scammed and wanted [REDACTED] money returned. [REDACTED] sent a total of five packages to [REDACTED], including four packages prior to March 3, 2021 containing cash and gift cards totaling \$6,000. [REDACTED] allegedly forwarded the money from those packages to [REDACTED]. The fifth package was delivered to Dinsmore on March 5, 2021, via priority mail. This package contained two counter checks totaling \$6,000 from [REDACTED] to [REDACTED]. [REDACTED] turned the two counter checks over to the FBI.

9. On March 4, 2021, Dinsmore received a package which contained \$900 cash from Minnesota resident [REDACTED] package was addressed to [REDACTED]. Dinsmore took possession of the package and stored it in the firm's safe. After her employment was terminated, [REDACTED] left [REDACTED] a voice message and requested that [REDACTED] send

██████ money to ██████. In addition, ██████ left ██████ a voice message and requested she forward the money to ██████.

10. On March 5, 2021, ██████ informed ██████ that ██████ employment had been terminated, and that the packages were ██████ personal business, which never should have been sent to Dinsmore. Dinsmore had alerted law enforcement because the transfer of money appeared to be an illegal scam. ██████ stated ██████ was not surprised by her statement. ██████ assured ██████ the transfer was not illegal, ██████ was just paying ██████ the money ██████ owed her.

11. Following the termination, ██████ cleaned out ██████ desk. Within the desk, ██████ found the following items: ██████ written records of incoming and outgoing packages with names, amounts, and addresses in different U.S. states and Ghana, Africa; approximately \$30,000 in used gift cards; and the two subject Devices: a black Kingston 4GB Data Traveler 4000 flash drive, and a black iPhone4s. Based on the records discovered, ██████ estimated ██████ received or sent out cash, gift cards, and goods totaling approximately \$186,000 on or about December 2018 through March 2021. The items from ██████ desk related to this matter were placed in a locked safe at Dinsmore prior to their release to the FBI.

12. On July 22, 2021, Dinsmore, through ██████, turned the Devices over to Special Agent Donald F. Bogardus III, who placed them in the evidence control room located at 425 W. Nationwide Blvd., in Columbus, Ohio. While the Federal Bureau of Investigation might already have the necessary authority to examine the Devices, I seek this additional warrant out of

an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and all applicable law.

13. The Devices are currently in the FBI's Evidence Control Room located at 425 W. Nationwide Blvd. Columbus Ohio, 43215. I know the Devices have been stored in a manner consistent with FBI Evidence collection policy and procedures.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

15. Based on my training, experience, and research, and from consulting the manufacturer’s advertisements and product technical specifications available online at

<http://support.apple.com> I know that the wireless telephone described in Attachment A has capabilities that allow it to serve as a digital storage device, world phone, digital camera, media player, mail attachment support, has wifi/cellular and internet access, and the USB storage device described in Attachment A has capabilities that allow it to serve as a digital storage device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

20. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A, wherever they may be found, to seek the items described in Attachment B.

REQUEST FOR SEALING

21. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



Aaron Beggs
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on April 12, 2022:



Kimberly A. Johnson
United States Magistrate Judge



ATTACHMENT A

1. The property to be searched is:
 - a. a black Kingston 4GB Data Traveler 4000 and
 - b. a black Apple iPhone 4s Model: A1387, FCC ID: BCG-E2430A which are currently in the custody of the FBI and located in the evidence control room located at 425 W. Nationwide Boulevard in Columbus, Ohio, 43215.
2. This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Money Laundering 18 U.S.C. 1956 and 1957 and involve [REDACTED] or [REDACTED] since January 1, 2018, including:

2. All information that constitutes fruits, contraband, evidence, and instrumentalities of violation of the Target Offenses involving the user(s) of the Devices.

3. Evidence of who used, owned, or controlled the Devices described in Attachment A;

4. All email (including drafts), text messages, SMS, MMS, iMessages, communications (including content) regarding, but not limited to:

- a. Financial Accounts
- b. Safe deposit boxes
- c. Identification documents

5. Any and all correspondence, records, documents, statements, cancelled checks, wire transfers, sales receipts, invoices, bills, checkbook registers, financial documents, or other material of any kind, relating to any bank accounts, investments accounts, financial accounts, loans, personal identifying information, and business activity. This includes, but is not limited to, correspondence, records, documents, statements, cancelled checks, checkbook registers, and other material of any kind relating or concerning [REDACTED]

6. All accounting, book keeping and financial records relating to receipts and expenditures including bank accounts, bank statements, credit card statements, records of accounts, records of income, journals, ledgers, financial statements, balance sheets, trial balances, statements of profits and losses, accounts and notes receivable, accounts and notes payable, check registers and canceled checks, cashier checks, wire transfer confirmations, federal, state, and local income tax returns including all schedules and attachments for drafts and filed returns, work papers, notes and memoranda, all tax records including tax preparation files, and documents relating to all other governmental filings or public statements.

7. Any and all paycheck stubs, receipts, K-1 reports, or other documents of any kind relating to any income earned, and/or expenses accrued.

8. Any and all identity documents and forms of any kind, including U.S. passports, VISAs and drivers licenses as well as foreign citizenship documents and forms including passports, VISAs, and drivers' licenses.

9. All documents relating to any and all transactions involving the proceeds of financial transactions, including, but not limited to, purchases and/or acquisitions of real and personal property including real estate homes, commercial buildings, aircraft, vehicles, jewelry, stocks, bonds, mutual funds, precious stones and metals, and any and all other articles of significant intrinsic value.

10. All calendars, appointment books, diaries, planners and contact lists or address books.

11. Any and all contracts, agreements, memoranda of understanding, billing statements, invoices, loan statements, receipts, marketing material, or written material of any kind indicating the purchase of goods and/or services.

12. Records and information relating to unlawfully obtaining, using or identifying information (PII);

13. Records and information constituting or relating to identification documents, including driver's licenses, social security cards, photo identification cards, and any device or image used in the fabrication of any identification document;

14. All telephone account records, to include without limitation account information, telephone numbers, bills, statements, transaction history/toll logs, and payments information.

15. All proceeds of the fraud, including any crypto-currency (in excess of \$100 dollars) or foreign currency worth in excess of \$100 dollars;

16. Records and information relating to travel (domestic and international), including but not limited to airline tickets, car rental agreements, commercial tickets, passports, and visas;

17. Records and information concerning indicia of use, ownership, possession, or control of the device including without limitation, IP logs, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

18. Keys, storage combinations, passwords and paperwork which indicate any other storage containers or facilities that could contain evidence of the scheme to defraud.

19. Records, letters, correspondence, chat logs, instant messages, faxes, and log files, and any and all computer storage media, which concerns or relates to:

- a. Correspondence, communication, or agreements related to the above scheme.
- b. Any and all passwords or commands that control access to any computer, files or data and,
- c. Any and all files, log files, data files and records relating to the use of internet service providers for purposes of committing the criminal offenses listed above;

20. Computer software, meaning any and all information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

21. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items, system documentation, and software and instruction manuals.

22. Computer passwords and data security devices, meaning any devices, programs, or data, whether in the nature of hardware or software, that can be used or designed to be used to restrict access to, or to facilitate concealment of, or destruction of any computer hardware,

computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form, and any evidence eliminator or data wiping software.

23. Browsing history, internet search history, email accounts and communication saved to each device, social media accounts and communications saved to each device, photographs, mms/SMS/ chat logs, cookies, documents;

24. Recorded telephone messages or conversations related to the criminal offenses listed above;

25. Immigration documents;

26. Evidence indicating the device owner's state of mind as it related to the crime under investigation;

27. All location history of the user of the device;

28. All credit card and other financial information including but not limited to bills and payment records;

29. All evidence of the times the device were used;

30. All passwords and encryption keys, and other access information that may be necessary to access the device and other associated accounts;

31. The identity of the person(s) who communicated with the device about matters relating to the above-mentioned violations, including records that help reveal their whereabouts.

32. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.